UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

2310 North Centennial Street, Suite 102, High Point, North Carolina 27265

Case No. 1:24MJ 341

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated by reference.

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C 1347	Health care fraud
18 U.S.C 1957	Engaging in monetary transaction in property derived from SUA

The application is based on these facts:

See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

In accordance with Rule 4.1(b)(2)(A), the Applicant appeared before me by telephone, was placed under oath, and attested to the contents of this Application, which was submitted to me by reliable electronic means.

/s/ David Yu
Applicant's signature

David Yu, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means).*

Date: 9/3/2024

Judge's signature

City and state: Winston-Salem, North Carolina

Hon. Joi Elizabeth Peake
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF THE PREMISES LOCATED AT 2310 North Centennial Street, Suite 102 High Point, NC 27265	Case No. 1:24MJ 341

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, David Yu, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since January 1999. I am currently assigned to a criminal investigations squad of the Charlotte Division where my duties include the investigation of matters involving health care fraud.

2. I am a "federal law enforcement officer" within the meaning of Rule 41(a) of the Federal Rules of Criminal Procedure. I have received extensive training related to health care fraud schemes. As a Special Agent, I have conducted or participated in numerous investigations of alleged violations of health care fraud and related statutes.

3. The information contained in this affidavit is known to me through involvement in the investigation, my background, training, and experience, and information provided by other individuals, investigators, and agencies involved in this investigation, including the Department of Health and Human Services – Office of Inspector General ("HHS-OIG").

4. This affidavit is made in support of an application to search the following location: 2310 North Centennial Street, Suite 102 High Point, NC 27265 ("SUBJECT PREMISES").

5. Based on my training and experience and the facts as set forth in this affidavit, I respectfully assert that there is probable cause to believe that violations of 18 U.S.C. § 1347 (Health Care Fraud) and 18 U.S.C. § 1957 (Conducting Transactions in Criminally Derived Property) (the "SUBJECT OFFENSES"), among others, have been committed by Chaudhry Ahmed and his companies – Dune Medical Supply, LLC and Prospect Health Solutions, Inc. I further submit that based on the evidence set forth below, and all reasonable inferences from that evidence, there is probable cause to believe that evidence, instrumentalities, and fruits of these violations, as more fully described in Attachment B, will be found on or in the SUBJECT PREMISES, as identified in Attachment A.

6. Because this affidavit is being submitted for the limited purpose of establishing probable cause for the issuance of a search warrant, it does not contain every fact known to me or other agents.

PROBABLE CAUSE

A. The Subject Offenses

7. Title 18 United States Code, Section 1347 prohibits health care fraud. "Whoever knowingly and willfully executes, or attempts to execute, a scheme or artifice—(1) to defraud any health care benefit program; or (2) to obtain, by means of false or fraudulent pretenses, representations, or promises, any of the money or property owned by, or under the custody or control of, any health care benefit program, in connection with the delivery of or payment for health care benefits, items, or services[,]" is guilty of health care fraud.

8. Title 18, United States Code, Section 1957 prohibits, "knowingly engag[ing] or attempt[ing] to engage in a monetary transaction in criminally derived property of a value greater than $10,000 and is derived from specified unlawful activity[.]"

B. Background on Medicare and Durable Medical Equipment

9. The Medicare Program is a federally funded health insurance program for eligible persons 65 years of age and older, and certain disabled persons, under which physicians, hospitals and other health care providers are compensated or reimbursed for covered medical services and supplies provided to Medicare beneficiaries. Medicare is a health care benefit program affecting commerce, as defined by Title 18, United States Code, Section 24(b).

10. Medicare is administered by the Centers for Medicare and Medicaid Services ("CMS"), which is an agency of the Department of Health and Human Services ("HHS").

11. Medicare is subdivided into multiple program "parts." Medicare Part A, for example, covers health care services provided by hospitals, skilled nursing facilities, hospices, and home health agencies. Medicare Part B covers physician and other licensed provider services and outpatient care, including an individual's access to durable medical equipment ("DME").

12. DME includes orthotic devices, such as knee braces, back braces, shoulder braces, wrist braces, and other devices. Under Medicare Part B, beneficiaries only receive Medicare-covered DME from "suppliers" that are enrolled in Medicare.

13. DME is equipment designed for repeated use and for a medical purpose, such as orthotic devices (including back, arm, and knee braces), wheelchairs, prosthetic limbs, collagen dressing, gauze, and hydrocolloid dressing.

14. Medicare reimburses DME companies for items and services rendered to beneficiaries. To receive payment from Medicare, providers must submit or cause the submission of claims to Medicare.

15. To enroll in Medicare Part B, DME suppliers are required to submit a completed enrollment also known as the "Form CMS-855S" to Medicare. The Form CMS-855S lists many standards necessary to obtain and retain Medicare billing privileges as a DME supplier.

16. The Form CMS-855S requires applicants to disclose to Medicare any individual or organization with an ownership interest, a financial interest, or managing control of a DME supplier. This includes anyone with 5% or more of an ownership stake, either direct or indirect, in the DME supplier; anyone with a partnership interest in the DME supplier, regardless of the percentage of ownership, any organizations with "managing control" over the DME supplier, as well as any and all "managing employees."

17. The form also requires the signature of an "authorized official" who certifies, among other things, that the DME supplier will abide by all Medicare laws, regulations, and instructions and not knowingly present or cause to be presented a false or fraudulent claim for payment by Medicare and will not submit claims with deliberate ignorance or reckless disregard of their truth or falsity.

18. A Medicare claim for DME reimbursement is required to set forth, among other things, the beneficiary's name and unique Medicare identification number, the equipment provided to the beneficiary, the date the equipment was provided, the cost of the equipment, and the name and unique physician or provider identification number of the provider who prescribed or ordered the equipment.

19. Medicare reimburses claims for DME only if the DME was medically necessary for the treatment of the beneficiary's illness or injury, prescribed by an appropriate medical provider, and actually provided to the beneficiary as billed.

20. The proper process involves examination of the patient by a physician or other appropriate licensed medical provider. After the examination, the provider is supposed to write a prescription for the beneficiary. The prescription should contain the patient's identifying information, the DME item that the treating provider believes is medically necessary for the patient, and the diagnosis codes relating the patient's medical condition. Absent a valid certification by the treating physician/provider, Medicare lacks the statutory authority to pay the claim.[1]

21. The prescription is then provided to the DME company, which provides the necessary equipment to the patient and submits a claim directly to Medicare for reimbursement.

22. The Healthcare Common Procedure Coding System ("HCPCS" codes) are published by the American Medical Association. The codes are part of a uniform coding system used to identify, describe, and code medical, surgical and diagnostic services performed by practicing physicians and other healthcare providers. DME suppliers use HCPCS codes to identify, describe and code equipment and materials that they supply. These codes are used to determine the reimbursement.

C. <u>The Relevant Parties</u>

23. Dune Medical Supply, LLC ("Dune") is a North Carolina corporation located at 2310 North Centennial Street, Suite 102 High Point, NC 27265 (SUBJECT PREMISES), that purportedly provides DME to Medicare beneficiaries.

---

[1] *See* 42 U.S.C. §§ 1395n(a)(2)(b) and 1395y(a)(1) ("No payment may be made…for any expenses incurred for items or services…which…are not reasonable and necessary for the diagnosis or treatment of illness or injury…").

24. Prospect Health Solutions, Inc. ("Prospect") is a Florida corporation located at 5460 North State Road 7, Fort Lauderdale, FL 33319, that purportedly provides DME to Medicare beneficiaries.

25. Chaudhry Ahmed was a resident of Guilford County and is the owner and registered agent of Dune and the owner and registered agent of Prospect. According to Medicare enrollment documents, Ahmed is listed on the Form CMS-855S as the owner of both Dune and Prospect. Ahmed electronically signed the document agreeing that he would not present, or cause to be presented, any false or fraudulent claim for payment to Medicare.

26. Records from the North Carolina Secretary of State reflect that Ahmed is the owner, manager, and registered agent of Dune and that Dune's mailing, principal, and registered office is 2310 North Centennial Street, Suite 102 High Point, NC 27265—the SUBJECT PREMISES.

27. Agents conducted surveillance at the SUBJECT PREMISES at least five times during August 2024. On multiple occasions, agents saw one car parked in front of the business. While conducting surveillance, agents saw signage at Suite 102 indicating that it was the business location of Dune Medical Supply. Most recently, an agent visited the SUBJECT PREMISES on August 30, 2024 and observed boxes stacked outside the door, as well as attempted delivery notices posted to the door.

28. On August 23, 2024, Ahmed was arrested pursuant to a criminal complaint issued in the United States District Court for the Middle District of North Carolina. *See* 1:24MJ313-1. A federal grand jury later returned an indictment against Ahmed. *See* 1:24CR263-1. As of the date of submission of this affidavit, Ahmed is in custody.

D. Probable Cause of the Fraudulent Scheme

29. From on or about April 27, 2024, through present, Medicare received complaints from hundreds of beneficiaries or providers claiming that Dune was fraudulently billing Medicare for DME that the beneficiaries never received, requested, needed or the provider never ordered. To date, over 580 complaints have been received related to Dune.

30. From on or about June 1, 2024, through present, Medicare received complaints from hundreds of beneficiaries or providers alleging that Prospect was fraudulently billing Medicare for DME that the beneficiaries never received, requested, needed or the provider never ordered. To date, over 450 complaints have been received related to Prospect.

Claims Analysis: Dune

31. A review of Medicare claims data revealed that Dune began submitting claims to Medicare around April 2024. Then from around April 2024 through around August 19, 2024, Dune submitted more than 36,000 claims for over 20,000 Medicare beneficiaries, resulting in claims reimbursement requests of over $56.3 million.

32. Data analysis showed that Medicare has approved disbursement of more than $15.4 million to Dune.

33. Of the total claims Dune submitted to Medicare, more than $54.1 million were billed to Medicare in the 60-day period ending August 19, 2024, which represented an increase of over 2,400% when compared to the previous 60 days. Based on my training and experience, I know that a significant increase in claim submission over a short period of time, as reflected in Dune's billings to Medicare can be indicative of fraud.

34. Furthermore, analysis of claims data showed that for approximately 67% of the claims Dune submitted, the beneficiary that allegedly received DME had no prior relationship with

the provider that allegedly ordered the DME. This is significant because, as explained, a DME order must be prescribed by an appropriate licensed medical provider based on the beneficiary's underlying condition. If a medical provider has no prior relationship with the beneficiary, it indicates the provider may not be one of the beneficiary's regular medical providers as well as they may not know whether the DME equipment was medically necessary. Based on my training and experience, I know that a high percentage of claims in which there is no prior relationship between the ordering provider and the beneficiary, as reflected in Dune's billings to Medicare, can be indicative of fraud.

35. Claims data also showed that approximately 75% of the beneficiaries on whose behalf Dune billed Medicare were identified in a separate investigation indicating that their identities were compromised and used unlawfully by individuals to obtain fraudulent reimbursements from Medicare. Based on my training and experience, compromised Medicare beneficiary information is shared or exchanged between fraudsters and is often used in subsequent fraudulent claim schemes.

36. Dune also submitted claims to Medicare for more than 115 beneficiaries who were deceased prior to the date of service listed on the claim. Several of those beneficiaries died more than three years before the date of service listed on the claim.

Claims Analysis: Prospect

37. A review of Medicare claims data revealed that Prospect began submitting claims to Medicare around May 2024. Then from around May 2024 through around August 19, 2024, Prospect submitted more than 28,000 claims for over 17,000 Medicare beneficiaries, resulting in claims reimbursement requests of over $45.6 million.

38. Data analysis showed that Medicare has approved disbursement of more than $11.6 million to Prospect.

39. Of the total claims Prospect submitted to Medicare, more than $45.1 million were billed to Medicare in the 60-day period ending August 19, 2024, which represented an increase of over 8,600% when compared to the previous 60 days.

40. Furthermore, analysis of claims data showed that for approximately 70% of the claims Prospect submitted, the beneficiary that allegedly received DME had no prior relationship with the provider that allegedly ordered the DME. The significance of this is explained in paragraph 34.

41. Claims data also showed that approximately 77% of the beneficiaries on whose behalf Prospect billed Medicare were identified in a separate investigation indicating that their identities were compromised and used unlawfully by individuals to obtain fraudulent reimbursements from Medicare.

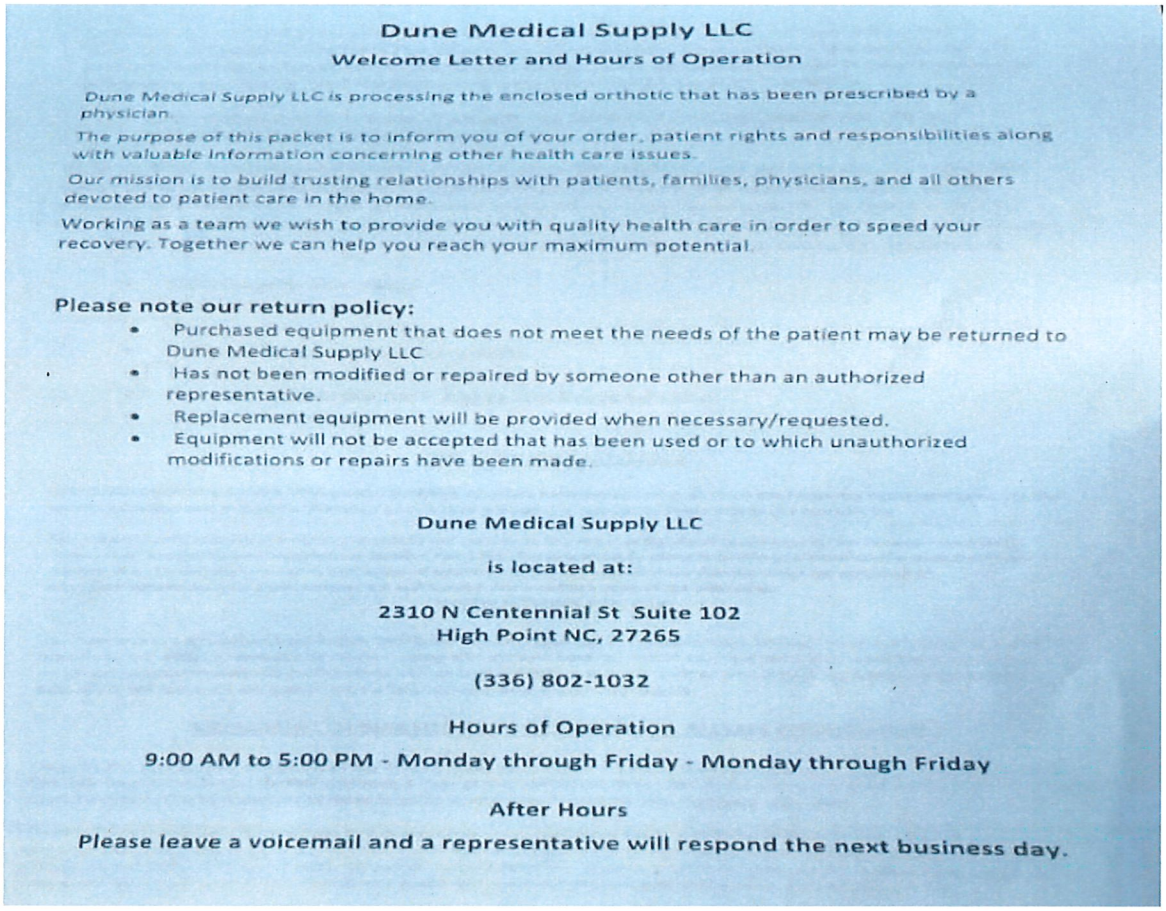
42. Prospect also submitted claims to Medicare for more than 50 beneficiaries who were deceased prior to the date of service listed on the claim. Several of those beneficiaries died more than three years before the date of service listed on the claim.

43. According to data analysis, Prospect submitted claims to Medicare for DME for at least 24 beneficiaries from Greensboro, North Carolina.

Interviews of Beneficiaries

44. Investigators interviewed numerous beneficiaries who submitted complaints to Medicare/HHS. For example, in or around July 2024, Dune submitted claims totaling approximately $1,963 to Medicare for a customized back brace (HCPCS L0637) purportedly provided to beneficiary, D.U.

45. Law enforcement officers interviewed K.G., daughter of Medicare beneficiary D.U. K.G. advised her mother, who resides in an assisted living facility, received a box containing a back brace. The box also contained documents which referenced Medicare would pay for it. D.U. informed K.G. that she did not order the brace. K.G. noted D.U. has suffered chronic back pain for a long time but does not do anything to treat it other than aspirin. K.G. provided photos of the brace, packaging, and documentation reflecting Dune's address at the SUBJECT PREMISES, as shown below:



Dune Medical Supply LLC

Welcome Letter and Hours of Operation

Dune Medical Supply LLC is processing the enclosed orthotic that has been prescribed by a physician.

The purpose of this packet is to inform you of your order, patient rights and responsibilities along with valuable information concerning other health care issues.

Our mission is to build trusting relationships with patients, families, physicians, and all others devoted to patient care in the home.

Working as a team we wish to provide you with quality health care in order to speed your recovery. Together we can help you reach your maximum potential.

Please note our return policy:

- Purchased equipment that does not meet the needs of the patient may be returned to Dune Medical Supply LLC
- Has not been modified or repaired by someone other than an authorized representative.
- Replacement equipment will be provided when necessary/requested.
- Equipment will not be accepted that has been used or to which unauthorized modifications or repairs have been made.

Dune Medical Supply LLC

is located at:

2310 N Centennial St Suite 102
High Point NC, 27265

(336) 802-1032

Hours of Operation

9:00 AM to 5:00 PM - Monday through Friday - Monday through Friday

After Hours

Please leave a voicemail and a representative will respond the next business day.

46. Similarly, around August 2024, Dune submitted claims totaling approximately $1,715 to Medicare for a back brace (HCPCS L0651) purportedly provided to beneficiary, K.D.

47. Law enforcement officers interviewed K.D. who confirmed she previously submitted a complaint regarding Dune. According to K.D., she received a box with no return label which contained a back brace. K.D. was not aware she was going to receive this brace because she does not have any problems with her back. She did not order the brace and believes her doctor would have called her if he had ordered it for her. K.D. attempted to contact Dune on two occasions. She left messages which were not returned.

48. Claims data revealed in or around July 2024, Dune submitted claims totaling approximately $4,397 to Medicare for a back brace and knee braces (HCPCS L0651, L2397, L1852) for Medicare beneficiary, T.P.

49. Law enforcement officers interviewed T.P. T.P. stated that he received a package that contained an invoice and several back and leg braces that he had not requested. T.P. stated that he contacted his physician regarding these braces and his doctor's nurse confirmed there had been no order for these braces from their office. T.P. stated that he called a company in High Point about returning the braces, and he was told that they had a piece of paper with his doctor's signature on it. The employee at this company told T.P. not to worry, the braces had already been paid for and there would be no expense to him. T.P. stated that there were two companies involved in the shipment of the braces and the company in High Point was not the same as the company listed on the package.

50. Medicare claims data also revealed in or around June 2024, beneficiary, S.L., received a back brace and knee braces totaling approximately $4,397 (HCPCS L0651, L2397, L1852).

51. Law enforcement officers interviewed the alleged prescribing physician, Dr. S.P. S.P. confirmed she was informed by patient, S.L., they had received a back brace and knee braces.

Dr. S.P. advised she did not order the braces and the patient does not have any medical problems which would necessitate a back brace or knee braces. Dr. S.P. does not recall receiving any phone calls or faxes asking her to sign an order for these items. Dr. S.P. noted she does not generally order braces as part of her practice.

52. Some beneficiaries who have filed complaints have also submitted copies of documents they received in the box containing DME from Dune. For example, one beneficiary shared a document that was enclosed with the DME that asked recipients to sign and return to the SUBJECT PREMISES a statement authorizing Dune to bill and receive payment from Medicare for the supplies they received.

Analysis of Activity in Bank Accounts

53. Investigators have obtained and reviewed information related to bank accounts in the name of Dune, Prospect, and Ahmed.

54. Medicare records show that Dune directed its claim reimbursements to a bank account at Truist Bank and that the SUBJECT PREMISES is listed as Dune's address. Investigation to date shows that Ahmed has access to the account.

55. The Truist records show that between May 7, 2024, and July 30, 2024, Medicare (including its contractors) deposited approximately $3,817,970 of claims reimbursement for DME into the account. And since July 30, 2024, Medicare records show that more than $9.8 million in additional reimbursements to Dune have been approved.

56. During this same period there were numerous wires from this account. One wire transfer was for approximately $45,000 to Faisal Khan LLC. An open-source search indicates that this company is a "boutique financial services consulting firm" specializing in cross border money transfers.

57. Medicare records show that Prospect directed its reimbursements to an account at JPMorgan Chase Bank. Bank records show that Ahmed has access to this account.

58. Between June 4, 2024 and August 21, 2024, Medicare deposited approximately $8.9 million of claims reimbursement for DME into the JPMorgan Chase Account.

59. The investigation identified approximately 24 wire transfers out of the JPMorgan Chase Account, including a $450,000 wire and $300,000 wire into an individual bank account at Bank of America in Ahmed's name.

E. Additional Probable Cause to Believe Evidence of the SUBJECT OFFENSES Will Be Found at the SUBJECT PREMISES.

60. Probable cause exists to believe that the evidence of the SUBJECT OFFENSES, as set forth in Attachment B, will be found within SUBJECT PREMISES, identified in Attachment A, as further described below.

61. As part of the investigation, agents interviewed Z.S. Z.S. reported that he worked at Dune's office at 2310 North Centennial Street, Suite 102, High Point, NC 27265 (the SUBJECT PREMISES) approximately once per week starting around early June 2024. Z.S. was hired by Chaudhry Ahmed, whom Z.S. understood to be the owner and manager of Dune. According to Z.S., Ahmed paid Z.S. approximately $40 to $50 in cash to clean Dune's office approximately once per week. Z.S. reported that he saw Ahmed working at Dune's office while he was cleaning, and that Ahmed would work in the first office on the left side of the hallway that leads from the front entrance of Suite 102. Z.S. reported that Ahmed worked on an Apple desktop computer that was located on the desk in his office. Z.S. said he would overhear Ahmed speaking on the phone with people who seemed to be patients.

62. On August 28, 2024, agents visited the office location of Dune at the SUBJECT PREMISES. The main entrance door was locked, the interior lights were off, and the business

appeared to be closed. Multiple attempted delivery stickers from UPS and FedEx were attached to the main entrance door. Multiple delivered packages were stacked at the exterior of the business near the main entrance door. Visible through the main entrance door was an Apple desktop computer on a desk in the first office on the left side of the hallway leading into the business, as shown below:

63. I know from training and experience that any provider, including providers of DME, who participate in the Medicare program are subject to a legal requirement to retain records. According to the Health Insurance Portability Act of 1996, health care providers must maintain medical and billing records related Medicare for at least six years. Accordingly, Dune is required to retain their medical records, and I believe medical records (or lack thereof) are evidence of criminal activity. Additionally, in order to retain an active Medicare enrollment, DME companies are required to maintain documentation for seven years under 42 C.F.R. 424.516(f)(A).

64. Based on my training and experience, I know that, in addition to physical files, medical records and correspondence about medical records and medical information are often stored electronically on computers and other electronic devices.

65. Based on my training and experience, I know that it is common for DME and associated companies to store beneficiary claim files and other business documentation in electronic format on computer systems. According to Medicare enrollment documents, Dune stores its medical records electronically.

Technical Terms

66. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Internet: The internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the internet, connections between devices on the internet often cross state and international borders, even when the devices communicating with each other are in the same state.

b. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

67. As described above and in Attachment B, this application seeks permission to search for records that might be found at the **SUBJECT PREMISES**, identified in Attachment A, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer, a computer's hard drive, or mobile device (e.g., a phone or tablet). Thus, the warrant

applied for would authorize the search and seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

68. *Probable cause*. I submit that if a computer or storage medium is found on the **SUBJECT PREMISES**, there is probable cause to believe those records would be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years for little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system

data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for this task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

69. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that forensic electronic evidence will be on any storage medium in the **SUBJECT PREMISES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence or business. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating, or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect.

For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it form law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer

and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

70. *Necessity of seizing or copying entire computers or storage media*. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of the storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination*. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine

storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of the data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements*. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the **SUBJECT PREMISES**. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. *Variety of forms of electronic media*. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

71. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant your affiant is applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

72. Any storage media that is determined to have been used to commit the Subject Offenses is an instrumentality of the crimes and thus will be seized and retained pursuant to the warrant. Further, any storage media that contains contraband will be seized and retained pursuant to the warrant.

CONCLUSION

73. Based on the forgoing, there is probable cause to believe that there is evidence, contraband, and/or instrumentalities as more particularly described in Attachment B to this affidavit.

This the 3 day of ~~August~~ September, 2024.

/s/ David Yu
David Yu
Special Agent
Federal Bureau of Investigation

In accordance with Rule 4.1(b)(2)(A), the Applicant appeared before me by telephone, was placed under oath, and attested to the contents of this Application, which was submitted to me by reliable electronic means.

this 3 day of ~~August~~ September, 2024.

Honorable Joi Elizabeth Peake
United States Magistrate Judge
Middle District of North Carolina

ATTACHMENT A
Place to be Searched

The place to be searched is the business office of Dune Medical Supply, LLC. Specifically, the placed to be searched is Suite 102 of the building located at 2310 North Centennial Street, High Point, North Carolina 27265.

The structure in which Suite 102 exists consists of a one-story building that is located on the east side of North Centennial Street and the west side of Eastchester Drive. The building has a brick façade and a gray shingled roof. There is a white arch over the entrance to Suite 102 and white columns on each side of the entrance.

Signage located at the North Centennial Street entrance to the building's parking lot reads "Dune Medical Supply" next to the number 102.

The entrance to Suite 102 faces the parking lot and is marked with "102" above the door. Signage on the door reads "Dune Medical Supply; Mon – Fri 9am – 4pm; 336-885-0115".

The photographs on the following pages depict the place to be searched:


2310
CENTENNIAL SQUARE
101
Chesson CPA, P.C.
104
ELEMENTS
HAIR SALON
102
DUNE
MEDICAL SUPPLY
105
103
LANA'S
ALTERATIONS
106
COLQUITT
LEASING INFORMATION 336-906-9401


102


102


102
DUNE
MEDICAL SUPPLY

ATTACHMENT B
Particular Things to be Seized

The things to be seized are fruits, evidence, and instrumentalities, in whatever form found, relating to violations of 18 U.S.C. § 1347 (Health Care Fraud) and 18 U.S.C. § 1957, including:

(1) Computers or other storage media, including cell phones, that could be used as a means to commit the violations described above or contain evidence or instrumentalities thereof.

(2) Durable medical equipment and delivery or return notices.

(3) Records and information referencing and revealing a scheme to defraud the Medicare or another health care benefit program.

(4) Records and information concerning the medical necessity (or lack thereof) and/ or delivery of DME items billed to a health care benefit program.

(5) Records and information referencing the filing for, receipt of, billing of, and deposit of insurance claims, including claims to Medicare, Medicaid, Tri-care, or any other health care benefit program.

(6) Patient/beneficiary billing records, itemized billing records, Explanation of Benefit forms, letters to patients explaining their bills, letters from patients inquiring about their bills, and any documents or memoranda concerning patient billings.

(7) Records and information reflecting beneficiary complaints and/or returns of DME products.

(8) Information and records of insurance training manuals, provider manuals, regulations, bulletins, reports, newsletters, notices, pamphlets, and correspondence related to proper billing and documentation procedures and any documentation regarding instructions for billing insurance providers/carriers.

(9) Information or records referencing beneficiary/patient medical or insurance information, beneficiary/patient lists, medical claims, or acquisition of patient identifying information.

(10) Patient/beneficiary medical records, including written documentation of verbal orders for DME; preliminary written orders for DME from treating physicians; detailed written orders for DME from treating physicians; or prescriptions for DME.

(11) All correspondence with insurance providers requesting supporting documentation, or alerts regarding billing and coding practices, including information related to any private and government insurance audits, audit findings, and/or results, as well as any documents related to overpayment recoveries.

(12) All marketing, public relations, or other promotional materials.

(13) All records of company training materials, manuals, marketing materials, policies, or directives relating to the administration of or billing for DME.

(14) Financial documents and records, including records of cryptocurrency, ledgers, check stubs or register, bank statements, loan applications, wire transfers, power of attorney, receipts, vouchers, invoices, journals, records of asset purchases or acquisitions, or diaries of financial information.

(15) Employment/Contractor records and personnel files.

(16) Records of control, including utility bills, telephone bills, rent or lease records showing ownership or control of the premises being searched; and records of control over other areas such as storage units where financial, medical, and other billing records may be maintained.

(17) Records and information referencing and revealing the location of proceeds from the Subject Offenses.

(18) For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

f. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

g. evidence of the times the COMPUTER was used;

h. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

i. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

j. records of or information about Internet Protocol addresses used by the COMPUTER;

k. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

As used above, the terms "documents," "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Precautionary instructions to preserve potential privileges:

If, during the execution of this warrant, the government discovers materials that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue its review. Prior to any further review, the Government will notify the Court of the need to establish a court-approved process for review and filtering of the potentially protected materials.